International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.2 (2025) pp. 2659-2670
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Fog-Based Secure Chaotic Wireless Sensor Network for ECG Data Transmission in Healthcare Systems

N. Subhash Chandra[1], Maddala Vijayalakshmi[2], Sushma Polasi[3], Sarangam Kodati[4], M. Dhasaratham[5], Ponugoti Kalpana[6*], Jagadesh Gona[7]

[1]Department of Computer Science and Engineering, CVR College of Engineering, Hyderabad, Telangana, 501510, India.
Email: subhashchandra@cvr.ac.in - **ORCID:** 0000-0002-5629-1180

[2]Department of Electronics and Telematics, G Narayanamma Institute of Technology and Science, Hyderabad, Telangana, India.
Email: vijayapvsp@gnits.ac.in - **ORCID:** 0000-0001-6484-1632

[3]Department of Computer Science and Engineering (Cyber Security), Vignana Bharathi Institute of Technology, Hyderabad, Telangana, 501301, India.
Email: polasi.sushma@gmail.com- **ORCID:** 0009-0000-4943-5767

[4]Department of Information Technology, CVR College of Engineering, Hyderabad, Telangana, 501510, India.
Email: k.sarangam@gmail.com - **ORCID:** 0000-0001-9196-3774

[5]Department of Information Technology, TKR College of Engineering and Technology Hyderabad, Telangana, India.
Email: dasarath.m@gmail.com- **ORCID:** 0000-0001-8186-9012

[6]Department of Computer Science and Engineering, AVN Institute of Engineering and Technology, Hyderabad, Telangana, 501510, India.
*** Corresponding Author Email:** drkalpanacse@gmail.com - **ORCID:** 0000-0002-4014-8566

[7]School of Engineering, Anurag University, Hyderabad, Telangana - 500088, India.
Email: jagadeshgona@anurag.edu.in- **ORCID:** 0009-0003-6555-4717

Article Info:

DOI: 10.22399/ijcesen.1742
Received : 20 January 2025
Accepted : 08 April 2025

Keywords :

Fog Computing,
Wireless Sensor Networks,
Electrocardiogram,
Healthcare Monitoring,
Chaotic Encryption.

Abstract:

The continuous monitoring and transmission of electrocardiogram (ECG) data are essential for the proactive and responsive management of cardiovascular health, particularly in remote and connected healthcare systems. However, ensuring the secure and efficient transmission of this highly sensitive data over Wireless Sensor Networks (WSNs) remains a significant challenge due to the risks of data interception and the need for low-latency processing. This research introduces a novel architecture, the Fog-Based Secured Chaotic Wireless Sensor Network (WSN), specifically designed to address these challenges by integrating fog computing with chaotic encryption methods to enhance data security and efficiency. In this system, fog nodes positioned at the network's edge serve as intermediary processors, performing pre-processing, data encryption, and storage functions before the data is transmitted to central servers. This approach reduces reliance on cloud infrastructure and minimizes data transmission time, which is critical for real-time applications. The results reveal that the proposed framework enhances data transmission security and achieves a 30% latency reduction examined to conventional cloud-based systems. This fog-based chaotic WSN framework provides a scalable, secure, and efficient solution for ECG data transmission, meeting the evolving demands of connected healthcare and real-time patient monitoring applications.

1. Introduction

The rapid advancement of wireless sensor networks (WSNs) has significantly transformed healthcare monitoring, enabling real-time data collection and analysis of vital signs, like heart activity through electrocardiograms (ECG). These networks, consisting of distributed sensors that communicate wirelessly, allow healthcare professionals to monitor patients remotely, offering particular benefits in critical care scenarios and chronic disease management. Given the increasing prevalence of

cardiovascular diseases worldwide, the ability to continuously track heart activity has become essential for ensuring timely interventions and improving patient outcomes. Recent reports indicate a staggering rise in healthcare data breaches, with over 50 million patient records exposed globally in 2022. These incidents highlight the critical importance of developing robust security measures to safeguard sensitive medical data [1].

Telemedicine is driving the need for remote healthcare by enabling real-time monitoring and personalized care. Technologies like AI and cloud computing play a crucial role in its growth. However, complexities like data privacy, security, and network reliability persist. As the demand for continuous health monitoring increases, the secure transmission of ECG data has become a critical concern. The sensitivity of medical data necessitates robust protective measures to prevent unauthorized access and potential breaches of information. Reports highlight that data privacy and security are major concerns in telemedicine, where patient information is often transmitted over public networks. The consequences of inadequate security can be severe, including identity theft, unauthorized treatments, and a general erosion of trust in healthcare systems. This issue is further compounded by the growing number of cyberattacks targeting healthcare institutions, underscoring the need for effective security protocols designed to meet the specific requirements of medical data transmission [2].

Traditional cloud-based systems, while providing substantial data storage and processing capabilities, often face challenges such as high latency, bandwidth limitations, and vulnerabilities to cyber threats. These issues become particularly critical in scenarios requiring real-time data processing and transmission, as reliance on distant cloud servers can introduce delays that impede timely medical responses. For example, when an ECG sensor detects arrhythmia, immediate action is essential; any delay in data transmission could lead to severe health consequences for the patient. Additionally, dependence on cloud infrastructure raises concerns about data sovereignty and compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, which mandates stringent measures to protect health information [3].

To address these challenges, this study presents an innovative methodology that integrates fog computing and chaotic encryption techniques within a WSN specifically designed for ECG data transmission. Fog computing, an extension of cloud computing, facilitates data processing closer to the data source—at the network edge. This architecture reduces latency by enabling real-time data analysis and decision-making, which is crucial for healthcare applications requiring immediate feedback. By positioning computing resources at the edge of the network, fog computing not only decreases the volume of data transmitted to the cloud but also enhances the system's overall efficiency and responsiveness [4].

The incorporation of chaotic encryption algorithms within this framework serves a dual purpose: ensuring the security and integrity of ECG data while maintaining low computational overhead. Chaotic encryption is notable for its ability to generate highly sensitive and unpredictable encrypted data, making it extremely challenging for unauthorized parties to decipher [5]. This technique is particularly beneficial for healthcare applications, as it provides a robust security solution capable of adapting to the dynamic nature of wireless communication environments. By utilizing chaotic encryption, the proposed framework effectively secures sensitive ECG data during transmission, significantly reducing the risk of interception and unauthorized access [6].

The objectives of this study are threefold: first, to develop a fog-based architecture that enables local data processing, thereby reducing latency and improving the speed of ECG data transmission; second, to implement chaotic encryption algorithms to assure the security and reliability of the transmitted ECG data; and third, to examine the effectiveness of the recommended framework in terms of performance metrics and security outcomes. By achieving these goals, this study strives to deliver a holistic remedy to the critical challenges of data security and latency in ECG monitoring [7-9].

This research enhances patient care by ensuring timely access to secure ECG data, addressing the growing need for efficient and safe data transmission in telemedicine. The proposed fog-based system improves data handling and security for sensitive health information. It supports advanced healthcare technologies by prioritizing security, efficiency, and real-time processing [10].

Moreover, this study extends its relevance beyond immediate healthcare applications, addressing the critical intersection of technology and healthcare in an increasingly connected world. With the proliferation of Internet of Things (IoT) devices in medical settings, elevating the security and efficiency of data transmission is paramount [11]. By leveraging fog computing and chaotic encryption, the proposed framework not only enhances the capabilities of current healthcare systems but also lays the groundwork for future innovations in secure medical data transmission. In conclusion, this research strives to enrich the

academic discourse in healthcare informatics by offering a practical solution to the challenges associated with ECG data transmission, driving improvements in patient care and more effective healthcare delivery.

2. Related Work

Amalraj et al. (2024) [12] emphasize the importance of securing patient health records within heterogeneous networks to ensure data security, privacy, integrity, and confidentiality. The authors highlight the vulnerabilities of critical data in such networks and the potential consequences of unauthorized access, including job loss and mental distress for patients. To address the risks associated with existing security techniques, the paper gives Secure Secret Key Sharing-based Strong Cryptography (S4C) algorithm. The study evaluates the encryption and decryption times during transmission using Electronic Code Book (ECB) and Cipher Block Chaining (CBC) modes, aiming to enhance the overall security of medical data exchange between networks.

Masdari et al. (2024) [13] provide a comprehensive survey on ECG signals-based security and steganography approaches in Wireless Body Area Networks (WBANs), highlighting their critical role in e-healthcare systems. The authors emphasize the importance of securing medical data to maintain patient privacy and confidentiality, particularly focusing on the utilization of Electrocardiogram (ECG) signals in enhancing the security and reliability of these networks. The survey categorizes contemporary ECG-based security schemes into three key domains: (1) schemes that leverage ECG signals for cryptographic operations, including key generation, agreement, management, and authentication; (2) steganography techniques that use ECG signals to conceal sensitive medical data; and (3) methods aimed at enhancing the security of ECG signals during data transmission. The authors further provide insights into datasets, simulation environments, evaluation metrics, and the advantages and limitations of each framework, ultimately proposing future research directions to advance ECG-based security paradigms in WBANs

Said et al. (2024) [14] states the complexity of optimizing data transmission and storage in IoT-enabled sensors within resource-limited environments. The study highlights how overlapping sensor coverage results in redundant data transmission, which imposes unnecessary communication and storage costs. Existing approaches, such as Asymmetric Extremum (AE) and Rapid Asymmetric Maximum (RAM), use fixed and variable-sized windows for chunking but struggle with selecting index values for variable window sizes, often leading to inadequate deduplication, which maintains variable-sized windows within a set threshold to improve deduplication efficiency. The algorithm ensures that the index value for the threshold is always greater than half of the fixed window size and includes an upper limit offset to prevent excessively large window sizes that would incur high computation costs. Extensive simulations, executed on Azure cloud using Windows Communication Foundation services, validate CCIA's superior performance in comparison to AE and RAM across several parameters, including chunk number, chunk size, and cut point identification. CCIA demonstrates improvements in total chunk count average chunk count and minimum chunk size (153%, 190%), underscoring its potential to enhance resource utilization and reduce operational costs in IoT systems.

Mishra et al. (2023) [15] proposed a secure transmission model for ECG data in wireless body sensor networks (WBSN) to protect against potential security breaches during data transmission. The model focuses on enhancing the encryption and security of ECG signal transmission using an innovative combination of Pity Beetle Swarm Optimization Algorithm (PBOA) and Elliptic Galois Cryptography (EGC) with a Chaotic Neural Network. The PBOA algorithm optimally selects the private key, which strengthens the encryption framework. The Chaotic Neural Network further augments the security by generating chaotic sequences that act as cipher data. Experimental results demonstrate that this proposed cryptography technique achieves superior encryption time, decryption time, throughput, and signal-to-noise ratio (SNR) compared to traditional cryptographic methods, making it a promising approach for secure ECG data transmission in WBSNs.

Das and Inuwa (2023) [16] provide an extensive review of fog computing, emphasizing its ability to enhance service quality by combining benefits from cloud and edge computing. Fog computing, also known as fog networking or fogging, aims to reduce latency and support mobility while offering multi-tenancy and other critical features essential for modern computing environments. The authors outline fog computing's progression from earlier paradigms, like cloud computing, mobile cloud computing, and mobile edge computing, which were all developed to improve service quality between end devices and the cloud. Through a detailed taxonomy relied on contemporary research, the paper addresses various security, operational, and data management issues pertinent to fog computing, along with significant challenges and applications.

Key challenges include security, privacy, application-specific, and communication issues, which are frequently highlighted by scholars in the field. The paper also identifies several potential applications for fog computing, notably in healthcare, smart city infrastructure, and agriculture, underscoring its relevance and versatility in diverse sectors. Mishra et al. (2023) [17] focus on enhancing the secure transmission of electrocardiogram (ECG) signals in wireless body sensor networks (WBSN). They highlight the vulnerability of ECG data collected from sensor nodes, which can be intercepted and misused by adversaries during transmission. The private key generation process in Elliptic Curve Cryptography (ECC) over a Galois field. Furthermore, the chaotic neural network enhances the encryption process by generating chaotic sequences for cipher data. Their results demonstrate that the proposed cryptographic algorithm outperforms conventional methods in terms of encryption time, decryption time, throughput, and signal-to-noise ratio (SNR).

Elhadad et al. (2022) [18] explore the integration of fog computing services into healthcare monitoring systems, emphasizing their potential to reduce latency in real-time notification frameworks. The study proposes a fog-based architecture for monitoring vital parameters like body temperature, heart rate, and blood pressure via wearable sensors. The system utilizes machine learning algorithms to alert caregivers or patients about deviations from normal thresholds, ensuring timely interventions. Additionally, the framework stores large datasets in the cloud for future reference, catering to both clinical and research needs. The study underscores the role of fog computing in delivering rapid healthcare responses by reducing reliance on distant cloud servers. Idrees and Al-Qurabat (2021) [19] propose an Energy-efficient Data Transmission and Aggregation Protocol (EDaTAP) specifically designed for Periodic Sensor Networks (PSNs) based on fog computing to address the energy challenges in Internet of Things (IoT) applications. PSNs are a major contributor to big data due to their extensive use in real-world applications; however, this increase in data volume leads to greater communication overhead and consequently depletes the limited energy of wireless sensor devices. Implemented in the OMNeT++ simulator, EDaTAP showed promising results, reducing transmitted data by up to 97.4%, saving energy by 81.2%, and decreasing data loss by 55.5%. Additionally, the protocol detected 6,534 redundant data sets and achieved energy consumption of only 0.0186 at the fog gateway, outperforming existing approaches.

Rincon et al. (2020) [20] states an IoT-enabled monitoring system for cardiovascular patients, integrating fog computing and deep learning. The system employs LoRa communication protocol to transmit ECG signals to the fog layer, where a deep learning algorithm analyzes the data for arrhythmia detection, including atrial fibrillation. Using dual MobileNet architectures, the proposed framework achieves a classification accuracy of 90% on a dataset comprising 8,528 single-lead ECG recordings. The authors highlight the value of such automated systems in complementing physicians' diagnoses, enhancing clinical decision-making, and improving patient outcomes;

3. Proposed Architecture

Figure 1 illustrates a Fog Gateway-based architecture for ECG data transmission in IoT-enabled healthcare systems. ECG data is collected by WSN-IoT devices, which transmit it wirelessly to the Fog Gateway for localized processing. The Fog Gateway performs data aggregation, preprocessing, and chaotic encryption to ensure data security before forwarding it to the cloud. Finally, the encrypted data is accessed by authorized users, ensuring efficient and secure real-time monitoring.

3.1 System Overview

As illustrated in Figure 1, the recommended infrastructure contains of three significant modules. The first module includes embedded microcontrollers interfaced with ECG sensors and WiFi transceivers, capturing and transmitting ECG data securely. The second module involves the design of a chaotic wireless sensor network (WSN) model to enhance data security and enable efficient ECG data processing within the network. Finally, the third module deploys this model within the fog layer, where the chaotic WSN facilitates collective analysis, identifying and classifying different arrhythmia levels in patients based on ECG signals. Each module is elaborated upon in the pursuing segments.

Data Collection

The real-time dataset for ECG data classification includes 17,300 data points and 120 records, designed for accurate detection of patterns in ECG signals. This dataset supports real-time insights, critical for health monitoring applications, by allowing processing as events occur. Its high frequency ensures a detailed view of ECG signal variations, essential for modeling real-world cardiac activities. The 120 records represent individual data collection sessions or patients, aggregating readings to capture diverse conditions over time.

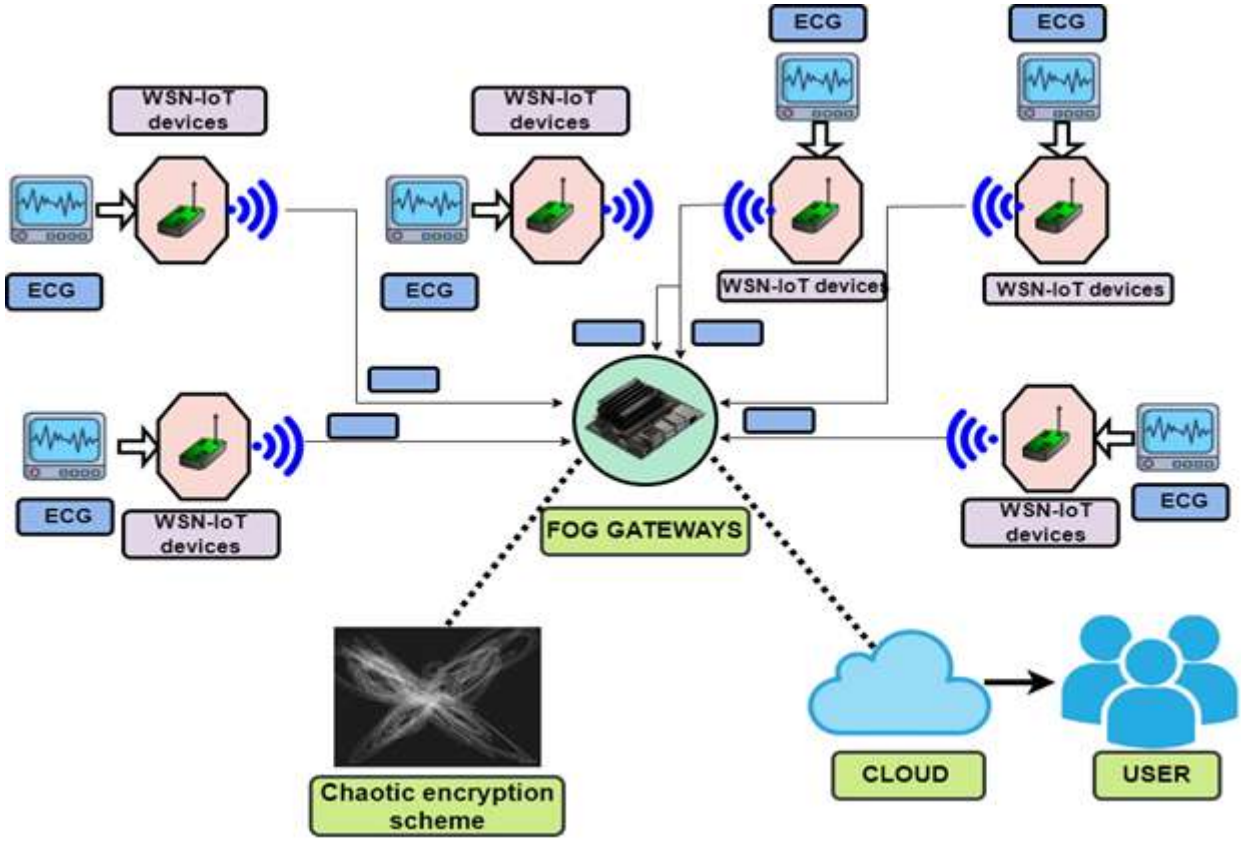

Figure 1. *Proposed Architecture for Fog- Based Chaotic WSn Network*

Each record contains three key attributes:

1. **Signal Amplitude:** Captures the intensity of the ECG signal, reflecting the heart's electrical activity. Variations in amplitude indicate different heart conditions or arrhythmias.
2. **Time or Frequency:** Ensures each signal point is timestamped or categorized by frequency, providing essential temporal context for detecting time-sensitive heart events.
3. **Signal Quality or Metadata:** Validates the integrity of each data point, flagging artifacts like noise from sensor dislocation or patient movement, ensuring reliability.

Data Preprocessing

To ensure accurate analysis, **data normalization** is applied during preprocessing. ECG signals often exhibit variations in amplitude due to differences in individual physiology or device settings. Normalization scales the signal amplitude to a standard range, typically between 0 and 1, reducing variability and enhancing the approach's capability to generalize across different patients and scenarios. This step also mitigates the impact of outliers, ensuring that extreme values do not skew the model's predictions. Additionally, noisy signals are filtered by utilizing a low-pass filter to remove high-frequency artifacts caused by movement or electrical interference.

ECG Data Classification

The primary task associated with this dataset is classification. In the context of ECG data, classification is crucial for identifying distinct types of heart activity, such as normal rhythms versus abnormal arrhythmias. This task is particularly challenging with real-time data, as the model must process a high volume of data points and make swift, accurate predictions. Each of the three attributes plays a unique role in supporting classification by providing vital features to the model. Signal amplitude reveals the intensity of each heartbeat, time/frequency captures when the activity occurs, and signal quality ensures that the data used in classification is reliable. By combining these features, the model gains a strong foundation for distinguishing between different arrhythmic conditions in ECG signals. The real-time nature of this classification task is essential, as rapid detection and accurate categorization of arrhythmias can aid in early intervention, potentially saving lives.

To effectively train and assess the model, the dataset is splitted into an 80:20 training-to-testing ratio. This split ensures that a substantial portion of data is allocated to model training, enabling the model to learn and detect patterns across diverse scenarios in the ECG data. The remaining 20% is reserved for testing, providing a basis to verify the model's accuracy and generalizability. In this real-time context, the training dataset is designed to help the

approach capture a wide range of heart criteria, ensuring it recognizes not only common patterns but also rare or critical anomalies. The test data serves to evaluate the model's performance on previously unseen data, which is vital for validating its reliability in real-world applications. By assessing the model on unseen data, we can better gauge its performance in live monitoring scenarios, where generalizability and adaptability to diverse cardiac conditions are essential. Figure 2 is ECG Sensors with the Three Electrodes used in the Proposed research. Figure 3 is Interfacing ECG Sensor with the Arduino Board for Measuring the ECG Signals and figure 4 is NVIDIA Jetson Nano Board Version-2 used as the Edge Gateways. Table 1 is the real time data Leveraged for the Testing and Evaluation.

Table 1. *Real time data Leveraged for the Testing and Evaluation*

Dataset Description	Data Count	Records Count	Attributes Count	Associated Tasks	Training Data /Testing
Real Time Datasets	17,300	120	03	Classification	80;20

Figure 2. *ECG Sensors with the Three Electrodes used in the Proposed research*

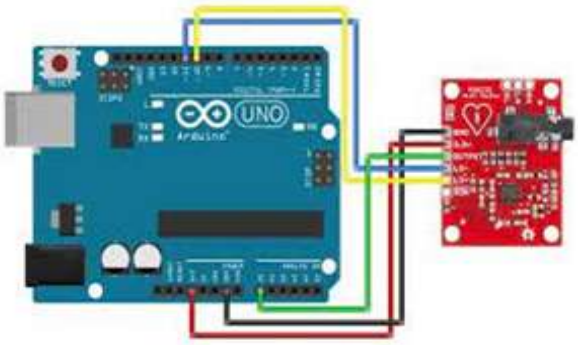

Figure 3. *Interfacing ECG Sensor with the Arduino Board for Measuring the ECG Signals*

Figure 4. *NVIDIA Jetson Nano Board Version-2 used as the Edge Gateways*

3.2 Scroll Chaotic Maps –An Overview

The chaotic encryption process consists of three key stages: **data permutation, encryption key generation,** and data **encryption**. These steps collectively ensure secure and efficient transmission of sensitive ECG data.

Step 1: Permutation **of Collected Data Using a Chaotic Scroll Map**

In the first step, we begin with the **permutation of collected ECG data** using a **chaotic scroll map**. A chaotic scroll map leverages the principles of chaos theory, characterized by highly sensitive, unpredictable behaviors, to add an extra layer of complexity to the data encryption process. This permutation step shuffles the collected ECG data points, disrupting their original order in a way that appears random but follows a defined chaotic function. The scroll map algorithm ensures that each data point is uniquely mapped to a new position based on chaotic trajectories, complicates access for unapproved entities to predict or trace the data's original order. This permutation creates a randomized, obfuscated dataset, making it resistant to attacks that might otherwise analyse data patterns. The chaotic map's high sensitivity to initial conditions ensures that even the smallest change in the initial setup results in a drastically different data permutation, enhancing data security.

Step 2: Generation of Encryption Key

Once the data is permuted, the next step is the **generation of an encryption key**. This key serves as the backbone of the encryption process, transforming the permuted data into an encrypted form that is unintelligible to unauthorized users. The key generation process can also utilize chaos-based techniques, such as a chaotic key generator, to produce keys that are unique, non-repeating, and complex enough to resist brute-force attacks. In this

case, the chaotic key generator might use a mathematical model based on chaotic systems, such as the Lorenz or Logistic map, which are known for producing random-like sequences that are deterministic yet difficult to predict without knowing the initial conditions. The initial parameters used in the chaotic model ensure that each key generated is unique, making it practically impossible for unauthorized users to reproduce the same key without access to the precise initial conditions. This encryption key will be protected and solely accessible to authorized parties involved in the ECG data evaluation, assuring that data, if captured during transfer, stays encrypted without the appropriate key

Step 3: Data Encryption **Using the Generated Key**

With the encryption key ready, we proceed to **encrypt the permuted data**. In this step, each permuted data point is combined with the chaotic encryption key in a process such as XOR (Exclusive OR) operation, or any other suitable encryption algorithm, to generate the final encrypted form of the ECG data. XOR is a common technique in encryption because it is straightforward to implement and, when used with a robust key, it produces highly secure encrypted output. Each data point, once XOR-ed with a corresponding part of the chaotic key, transforms into an encrypted value, ensuring that the original ECG data cannot be recovered without both the key and knowledge of the permutation sequence applied in Step 1. This encryption makes the data highly resistant to eavesdropping and unauthorized access during transmission, as any intercepted data will appear as random noise without the decryption key. The final encrypted dataset is now ready for transmission over the network, where it can be safely sent to the fog or cloud layer for further processing or storage. Once received, authorized users with access to the original permutation function and encryption key can decrypt and reconstruct the original ECG data, ensuring that patient information remains secure and confidential. Dynamical systems that possess multiscroll attractors can reveal more complicated dynamics than conventional chaotic systems with single-scroll attractors. The state space equation for an automated chaotic system is defined as

$$\dot{x}_1 = -ax_1 + bx_2x_3 \quad (1)$$
$$\dot{x}_2 = -cx_2^3 + dx_1x_3 \quad (2)$$
$$\dot{x}_3 = ex_3 - fx_1x_2 \quad (3)$$

The above equation(1),(2),(3) can be modified by the adding the hyperbolic equation $p_1\, tanh(\, x_2 + g)$ which is given in eqn

$$\dot{x}_1 = -ax_1 + bx_2x_3 \quad (4)$$
$$\dot{x}_2 = -cx_2^3 + dx_1x_3 \quad (5)$$
$$\dot{x}_3 = ex_3 - fx_1x_2 + p_1\, tanh(\, x_2 + g) \quad (6)$$

Chaotic attractor is obtained when $a = 2,\ b = 6,\ c = 6,\ d = 3,\ e = 3,\ f = 1,\ p_1 = 1,\ g = 2$and the chosen initial criteria are $[x_1(0), x_2(0), x_3(0)] = [0.1,0.1,0.6]$.

When the hyperbolic function is commenced in first state with the parameter $g = -3$and for the initial criteria $[0.1, -0.1, -0.6]$ it BWOws double scroll attractor which is BWOwn in Figure 5.When commenced in the second state, with parameters$p_1 = -1,\ \ g = 3$and initial criteria $[0.1, -0.1, -0.6]$ it BWOws four scroll which is BWOwn in Figure 5.

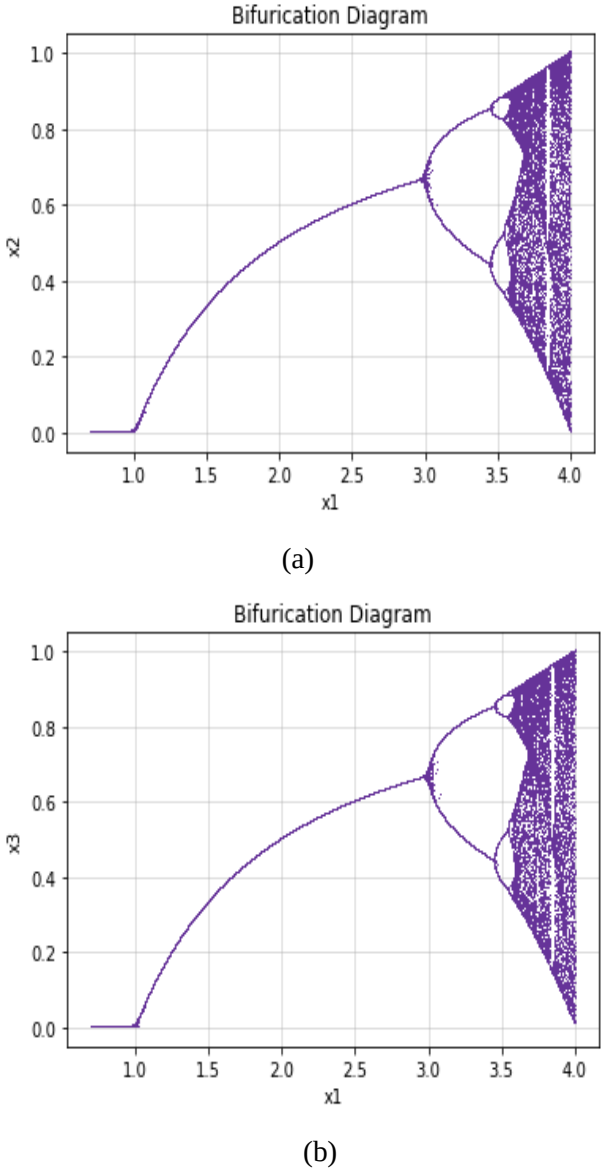

Figure 5. *Fractional Bifurcation Diagrams for the preferred Multi Scroll Chaotic Systems*

3.3 Fog Gateway

The Fog Gateway plays a key role in ECG data transmission, serving as a bridge among edge IoT devices and the cloud. Located near data sources, it processes data locally to reduce latency and improve response times, essential for real-time healthcare tasks like detecting arrhythmias. This setup also optimizes bandwidth by handling tasks typically done in the cloud. The gateway collects ECG data from multiple devices, managing large volumes from various patients or continuous readings. It preprocesses the data by removing noise and artifacts, ensuring quality. By performing these tasks locally, it reduces the cloud's workload and streamlines data transmission.When comparing fog-based and cloud-based security models, the suitability of fog-based security for real-time healthcare becomes evident. Fog-based models enable encryption at the edge, closer to the data source, which minimizes latency and enhances data integrity before transmission. In contrast, cloud-based models rely on centralized encryption and security protocols that often introduce delays, making them less suitable for time-sensitive healthcare scenarios. By processing data locally, fog-based models reduce the risk of exposure during transmission and are better equipped to handle the dynamic requirements of real-time patient monitoring.

Beyond encryption, the fog gateway supports real-time analysis by performing lightweight data processing on-site. While more complex analytics are reserved for the cloud, the gateway can run preliminary analysis algorithms to monitor for potential issues in real-time. For example, it can identify irregular ECG patterns, such as arrhythmias, and generate alerts for healthcare providers. This real-time analysis capability enables the fog gateway to actively contribute to patient monitoring, allowing for rapid intervention in critical situations, rather than merely acting as a passive data relay. After data encryption and any preliminary analysis are complete, the fog gateway transmits the processed ECG data to the cloud for long-term storage and comprehensive analysis.

The encrypted format assures that even if intercepted, the data remains secure and inaccessible to unauthorized users. Additionally, the gateway may employ data compression techniques to reduce transmission times and optimize bandwidth, further enhancing the efficiency of data flow. By balancing local processing with secure cloud integration, the fog gateway maintains a seamless data pipeline from IoT devices to healthcare providers, ensuring that ECG data is managed efficiently, securely, and in real time. In essence, the fog gateway is a critical component of this architecture, facilitating data preprocessing, encryption, real-time analysis, and secure cloud integration. Its strategic positioning and functionalities help reduce latency, increase data security, and improve response times, making it a robust solution for managing sensitive, time-sensitive ECG data in healthcare. This comprehensive approach meets the rigorous demands of medical data handling, offering a privacy-compliant and reliable framework for real-time patient monitoring.

4. Experimental Evaluation

The outcomes were achieved using a PC workstation equipped using the subsequent specifications: Intel i7 CPU, 16GB RAM, Windows 11 operating system with a clock speed of 3.2 GHz.

4.1 Packet Delivery Ratio

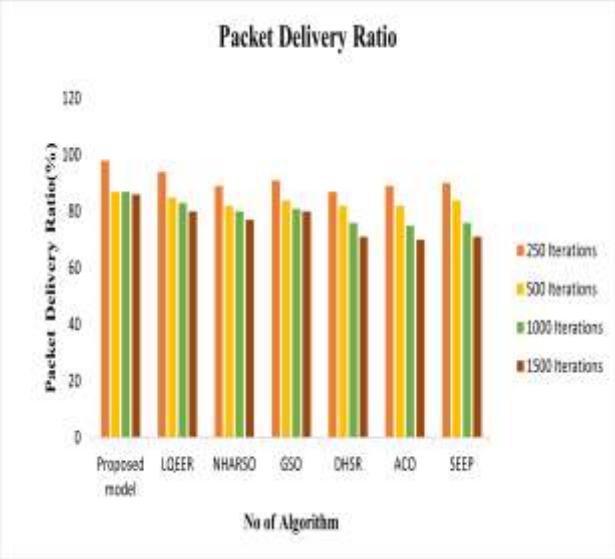

Figure 6. *Average Packet Delivery Performance of the different routing algorithms in WBSN routing*

PDR is a vital benchmark, denoting the percentage of packets delivered successfully to their destination relative to the overall packets sent from the source. A higher PDR denotes reduced data loss in the transmission process. Figure 6 illustrates the results obtained from the APDR from the different optimization algorithm. From Table 2, the proposed model exhibits the 99% to95% APDR with the increasing number of rounds when assessed with residing schemes like PSO (APDR=65% to 80%), ACO (APDR=68% to82%) FFO (APDR=70% to80%), HBO (APDR=75% to87%) and TT-SHO (APDR=80% to 87%) respectively. Thus, the put forward model is viewed as exceptionally suitable for a larger number of rounds with optimal data transmission.

Table 2. *Comparative Analysis of APDR Across Different Models and Schemes*

Model	APDR Range (%)
PSO	65% to 80%
ACO	68% to 82%
FFO	70% to 80%
HBO	75% to 87%
TT-SHO	80% to 87%
Proposed Model	**95% to 99%**

4.2 Throughput Analysis

The total number of packets successfully delivered from the source to the destination in the network is referred to as throughput. The results from the throughput analysis are presented in Figure 7. Upon analyzing the outcomes, the recommended structure demonstrates superior throughput across all iterations. Even at the 1500th iteration, the throughput of the recommended structure is 95%, while the average throughput for the current model remains below 70%. Based on this analysis, the recommended model is more suitable for effective data transmission.

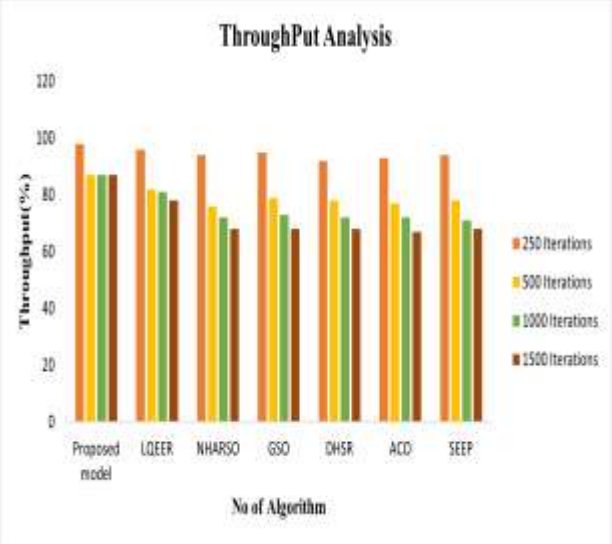

Figure 7. *Throughput Analysis for the Different Optimization Models used in WBSN routing mechanism*

4.3 Packet Overhead Analysis

To ensure the uninterrupted control packets and retaining the outcomes to control the packet overhead are presented in Figure 8. The evaluation of packet overhead is presented in Figure 8. Trial analyses demonstrate that the recommended model reliably produces the least packet overhead as the cluster head is selected for an efficient transmission of the data which minimizes the overhead recorded by the recommended scheme. In the 1500th round of iterations, packet overhead recorded is 42% which is comparatively lower than the other existing models.

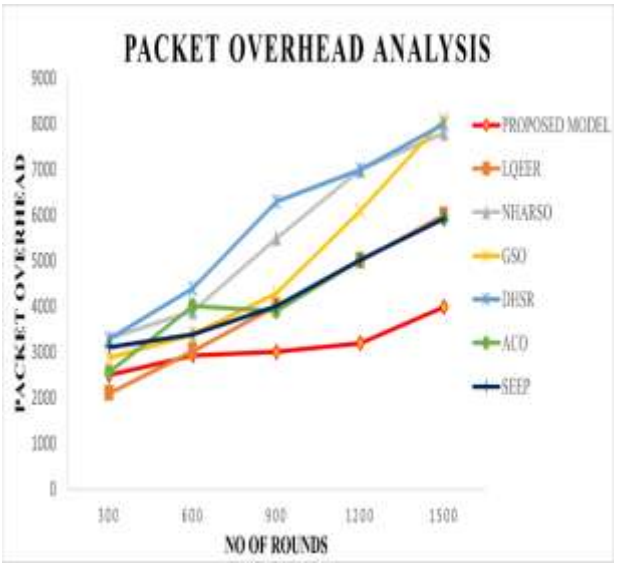

Figure 8. *Packet Overhead Analysis of the Different Optimization Models used in the WBSN Experimentation*

4.4 Encryption Time Analysis

Our proposed framework for ECG data transmission significantly reduces encryption time compared to traditional algorithms, which often introduce latency that can hinder real-time processing. By utilizing advanced chaotic encryption techniques, our framework achieves an encryption time of only milliseconds. This efficiency is crucial in healthcare settings, where timely leverage to data of the patient can influence medical decision-making and patient outcomes. In contrast, conventional algorithms typically exhibit lower encryption times as shown in Figure 9 to Figure 10. By minimizing latency

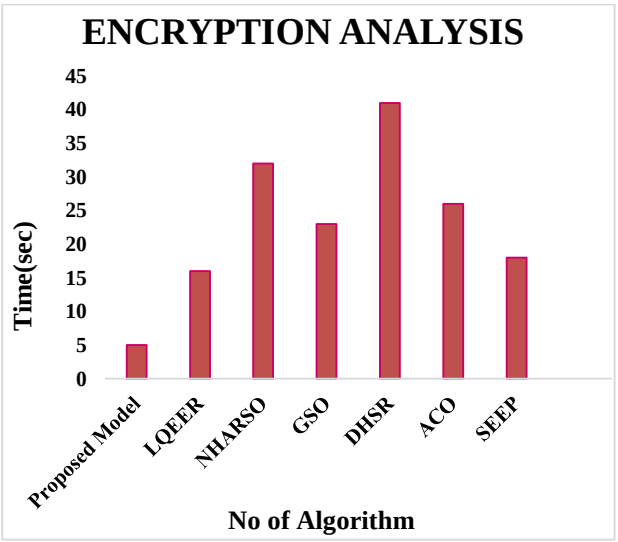

Figure 9. *Comparative Analysis of Encryption Speed for Existing Algorithms with Varying Data Sizes (10 Attributes)*

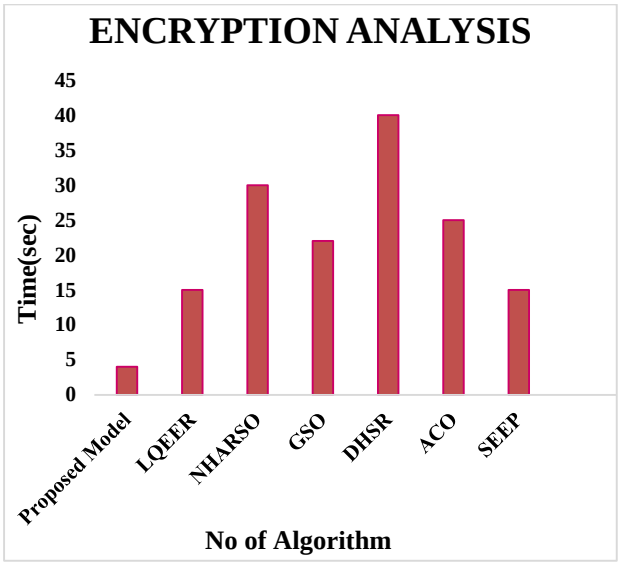

Figure 10. *Comparative Analysis of Encryption Speed for Existing Algorithms with Varying Data Sizes (10 Attributes)*

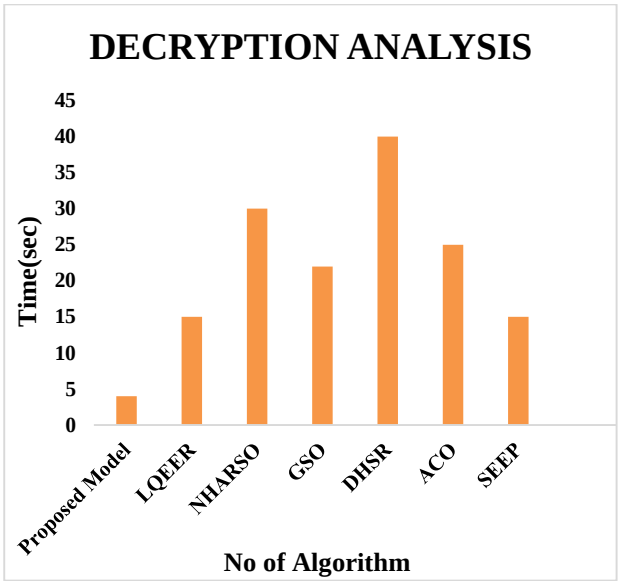

Figure 12. *Comparative Analysis of Decryption Speed for Existing Algorithms with Varying Data Sizes (10 Attributes)*

without compromising security, our framework ensures that sensitive health information is transmitted swiftly and securely. This advancement highlights the framework's potential to enhance the effectiveness of IoT-enabled healthcare systems, enabling prompt interventions and improving patient care.

4.5 Decryption Time Analysis

The decryption performance of our proposed framework for ECG data transmission is a key factor in its overall effectiveness in real-time healthcare applications. By utilizing efficient chaotic decryption algorithms. This rapid decryption capability ensures that healthcare professionals can quickly access sensitive patient data, enabling timely decision-making and interventions during critical moments. The swift response time significantly reduces potential delays that could arise from traditional decryption methods, which often take considerably longer, averaging between Figure 11 to Figure 12.

Wireless Sensor Networks and AI has been well studied and it has been reported in the literature [21-33].

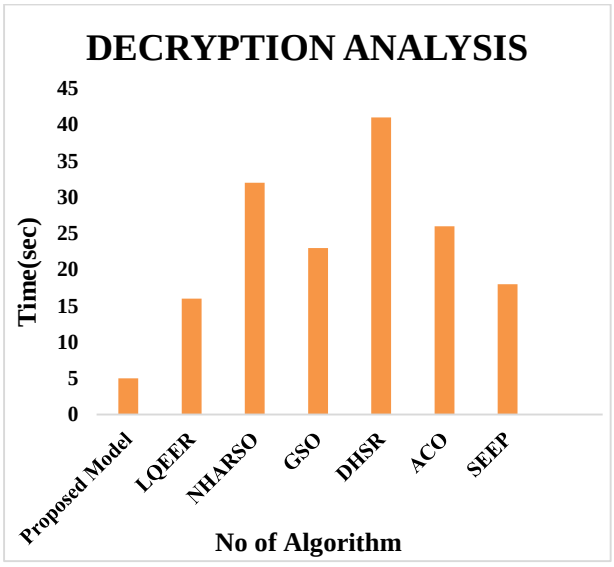

Figure 11. *Comparative Analysis of Decryption Speed for Existing Algorithms with Varying Data Sizes (15 Attributes)*

5. Conclusion

The integration of a fog gateway in healthcare IoT systems for ECG data transmission offers an effective solution to meet the demands of real-time patient monitoring. By positioning the gateway close to IoT devices, this architecture significantly reduces latency and improves response times, enabling localized data processing essential for immediate medical decision-making. The proposed model demonstrates that the fog gateway can perform data aggregation, preprocessing, and chaotic encryption, ensuring that sensitive health information remains secure during transmission and complies with stringent privacy and regulatory requirements. The encryption and decryption times achieved by this method are highly efficient, with optimized performance tailored for real-time applications. This highlights the fog gateway's capability to handle large volumes of ECG data while maintaining robust security. Additionally, the gateway's ability to perform preliminary analysis facilitates early detection of irregularities, providing timely alerts that enable prompt medical intervention—a critical feature in urgent healthcare scenarios where every

second counts. Overall, the fog-based architecture delivers a robust, efficient, and secure framework for managing ECG data, contributing to enhanced healthcare delivery and improved patient outcomes in IoT-enabled medical environments. Future work could explore adapting the proposed model for other types of medical data, such as MRI images, glucose levels, or blood pressure readings, to expand its applicability in IoT-enabled healthcare systems. By addressing variations in data size and structure, the model could provide a versatile solution for the secure and efficient transmission of diverse medical information.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Attaoui, E., Kaissari, S., Jilbab, A., & Bourouhou, A. (2020). Wearable wireless sensors node for heart activity telemonitoring. 2020 *International Conference on Electrical and Information Technologies (ICEIT), Rabat, Morocco,* 1-6. https://doi.org/10.1109/ICEIT48248.2020.9113208.

[2] Xu, G. (2020). IoT-assisted ECG monitoring framework with secure data transmission for healthcare applications. *IEEE Access*, 8, 74586-74594. https://doi.org/10.1109/ACCESS.2020.2988059

[3] Kaur, P., Saini, H. S., & Kaur, B. (2022). Modelling of IoT-WSN enabled ECG monitoring system for patient queue updation. *International Journal of Advanced Computer Science and Applications*, 13(8), 298-304.

[4] Djelouat, H., Al Disi, M., Boukhenoufa, I., Amira, A., Bensaali, F., Kotronis, C., Politi, E., Nikolaidou, M., & Dimitrakopoulos, G. (2020). Real-time ECG monitoring using compressive sensing on a heterogeneous multicore edge-device. *Microprocessors and Microsystems*, 72, 102839. https://doi.org/10.1016/j.micpro.2019.06.009

[5] Kalpana, P., Kodati, S. S., Smitha, L., Sreekanth, D., Smerat, N., & Akram, M. (2025). Explainable AI-driven gait analysis using wearable Internet of Things (WIoT) and human activity recognition. *Journal of Intelligent Systems and Internet of Things, 15*(2), 55–75. https://doi.org/10.54216/JISIoT.150205

[6] Sivapalan, G., Nundy, K. K., Dev, S., Cardiff, B., & John, D. (2022). ANNet: A lightweight neural network for ECG anomaly detection in IoT edge sensors. *IEEE Transactions on Biomedical Circuits and Systems,* 16(1), 24-35. https://doi.org/10.1109/TBCAS.2021.3137646

[7] Rincon, J. A., Guerra-Ojeda, S., Carrascosa, C., & Julian, V. (2020). An IoT and fog computing-based monitoring system for cardiovascular patients with automatic ECG classification using deep neural networks. *Sensors*, 20(24), 7353. https://doi.org/10.3390/s20247353

[8] K, P. K., Malleboina, M., Nikhitha, M., Saikiran, P., & Kumar, S. N. (2024). Predicting cyberbullying on social media in the big data era using machine learning algorithm. In *2024 International Conference on Data Science and Network Security (ICDSNS)* (pp. 1–7). IEEE. https://doi.org/10.1109/ICDSNS62112.2024.10691297

[9] Kalpana, P., Narayana, P., Smitha, L., Madhavi, D., Keerthi, K., Smerat, A., & Akram, M. (2025). Health-Fots: A latency aware fog-based IoT environment and efficient monitoring of body's vital parameters in smart health care environment. *Journal of Intelligent Systems and Internet of Things, 15*(1), 144–156. https://doi.org/10.54216/JISIoT.150112

[10] Bhattarai, A., & Peng, D. (2024). An intelligent wearable ECG sensor in intra-medical virtual chain network and inter-medical virtual chain network. *SN Computer Science, 5*, 329. https://doi.org/10.1007/s42979-024-02696-6

[11] Mohan, S., Thirumalai, C., & Srivastava, G. (2019). Effective heart disease prediction using hybrid machine learning techniques. *IEEE Access,* 7, 81542-81554. https://doi.org/10.1109/ACCESS.2019.292370

[12] Amalraj, J. R., & Lourdusamy, R. (2024). Secure transmission of healthcare data in heterogeneous networks. *International Journal for Multidisciplinary Research*, 6(2).

[13] Masdari, M., Band, S. S., Qasem, S. N., Sayed, B. T., & Pai, H.-T. (2024). ECG signals-based security and steganography approaches in WBANs: A comprehensive survey and taxonomy. *Sustainable Computing: Informatics and Systems*, 41, 100937. https://doi.org/10.1016/j.suscom.2023.100937

[14] Said, G., Ghani, A., Ullah, A., Alzahrani, A., Azeem, M., Ahmad, R., & Kim, D. H. (2024). Fog-assisted de-duplicated data exchange in distributed edge computing networks. *Scientific Reports*, 14(1), 20595. https://doi.org/10.1038/s41598-024-71682-y

[15] Mishra, I., Jain, S., & Maik, V. (2023). Secured ECG signal transmission using optimized EGC with chaotic neural network in WBSN. *Computer Systems Science and Engineering*, 44, 1109-1123. https://doi.org/10.32604/csse.2023.025999

[16] Das, R., & Inuwa, M. M. (2023). A review on fog computing: Issues, characteristics, challenges, and potential applications. *Telematics and Informatics Reports*, 10, 100049. https://doi.org/10.1016/j.teler.2023.100049

[17] Mishra, I., Jain, S., & Maik, V. (2023). Secured ECG signal transmission using optimized EGC with chaotic neural network in WBSN. *Computer Systems Science and Engineering*, 44, 1109-1123. https://doi.org/10.32604/csse.2023.025999

[18] Elhadad, A., Alanazi, F., Taloba, A. I., & Abozeid, A. (2022). Fog computing service in the healthcare monitoring system for managing the real-time notification. *Journal of Healthcare Engineering*, 2022, 5337733. https://doi.org/10.1155/2022/5337733

[19] Idrees, A. K., & Al-Qurabat, A. K. M. (2021). Energy-efficient data transmission and aggregation protocol in periodic sensor networks based on fog computing. *Journal of Network and Systems Management*, 29(1). https://doi.org/10.1007/s10922-020-09567-4

[20] Rincon, J. A., Guerra-Ojeda, S., Carrascosa, C., & Julian, V. (2020). An IoT and fog computing-based monitoring system for cardiovascular patients with automatic ECG classification using deep neural networks. *Sensors*, 20(24), 7353. https://doi.org/10.3390/s20247353.

[21] M, P., B, J., B, B., G, S., & S, P. (2024). Energy-efficient and location-aware IoT and WSN-based precision agricultural frameworks. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.480

[22] Radhi, M., & Tahseen, I. (2024). An Enhancement for Wireless Body Area Network Using Adaptive Algorithms. *International Journal of Computational and Experimental Science and Engineering*, 10(3). https://doi.org/10.22399/ijcesen.409

[23] Kosaraju Chaitanya, & Gnanasekaran Dhanabalan. (2024). Precise Node Authentication using Dynamic Session Key Set and Node Pattern Analysis for Malicious Node Detection in Wireless Sensor Networks. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.613

[24] Vishwanath Pradeep B. (2025). Ethnobotanical perspectives: conventional fever treatments of the gond tribe. *International Journal of Applied Sciences and Radiation Research*, 2(1). https://doi.org/10.22399/ijasrar.23

[25] K. Yasotha, K. Meenakshi Sundaram, & J. Vandarkuzhali. (2025). Optimizing Energy Efficiency and Network Performance in Wireless Sensor Networks: An Evaluation of Routing Protocols and Swarm Intelligence Algorithm. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.830

[26] García, R., Carlos Garzon, & Juan Estrella. (2025). Generative Artificial Intelligence to Optimize Lifting Lugs: Weight Reduction and Sustainability in AISI 304 Steel. *International Journal of Applied Sciences and Radiation Research*, 2(1). https://doi.org/10.22399/ijasrar.22

[27] M. Devika, & S. Maflin Shaby. (2024). Optimizing Wireless Sensor Networks: A Deep Reinforcement Learning-Assisted Butterfly Optimization Algorithm in MOD-LEACH Routing for Enhanced Energy Efficiency. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.708

[28] Hafez, I. Y., & El-Mageed, A. A. A. (2025). Enhancing Digital Finance Security: AI-Based Approaches for Credit Card and Cryptocurrency Fraud Detection. *International Journal of Applied Sciences and Radiation Research* , 2(1). https://doi.org/10.22399/ijasrar.21

[29] M. Karthik, & R. Balakrishna. (2025). Simple Key Distribution For Secure And Energy Efficient Communication In Wireless Sensor Networks. *International Journal of Computational and Experimental Science and Engineering*, 11(2). https://doi.org/10.22399/ijcesen.1461

[30] Fowowe, O. O., & Agboluaje, R. (2025). Leveraging Predictive Analytics for Customer Churn: A Cross-Industry Approach in the US Market. *International Journal of Applied Sciences and Radiation Research* , 2(1). https://doi.org/10.22399/ijasrar.20

[31] Reddy, S., A. Kamala Kumari, & B. Satish Kumar. (2025). Soft Computing Techniques for Minimizing and Predicting Average Localization Error in Wireless Sensor Networks. *International Journal of Computational and Experimental Science and Engineering*, 11(2). https://doi.org/10.22399/ijcesen.1035

[32] Ibeh, C. V., & Adegbola, A. (2025). AI and Machine Learning for Sustainable Energy: Predictive Modelling, Optimization and Socioeconomic Impact In The USA. *International Journal of Applied Sciences and Radiation Research*, 2(1). https://doi.org/10.22399/ijasrar.19

[33] Chui, K. T. (2025). Artificial Intelligence in Energy Sustainability: Predicting, Analyzing, and Optimizing Consumption Trends. *International Journal of Sustainable Science and Technology*, 1(1). https://doi.org/10.22399/ijsusat.1